ABSTRACT

A method and system for generating a pseudo-random bit series based on a given polynomial of order N, for M parallel communication lines using a machine comprising: N flip-flop machines and logic circuit . The flip-flop machines is initialized according to a given series of N bits. The logic circuit calculates a series of the next M+N bits using the N flip flop machines as function of the current N bit series wherein the function is based on two pre-generated equations. These equations are generated by recursive calculation of matrix array of order N*M according the given polynomial equation.